DO NOT ENTER: /JT/

05/19/2008



**IN THE CLAIMS**

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method for automated adaptive reprovisioning of servers under security assault, the method comprising:

detecting a security assault or a possible security assault on a first server;

incrementing a counter associated with the first server to account for the security assault or possible security assault;

notifying a human operator if a value of said counter exceeds a maximum limit;

and

reprovisioning by automatically creating a new server instance with a ~~desired~~ new server configuration to perform at least one of the tasks performed by said first server, if said value of said counter does not exceed the maximum limit, wherein said ~~desired~~ new server configuration for said new server instance is selected from a table comprising a plurality of new server configurations ~~available for said first server~~ , said new server configuration being associated in said table with said value of said counter.

2. (Original) The method of claim 1, wherein said detecting comprises determining if said first server is a candidate for reprovisioning, because of properties or behavior that suggest its security has been compromised or is likely to be compromised, or its functioning otherwise unacceptably impaired, by a security assault.

3. (Original) The method of claim 1, wherein said reprovisioning comprises automatically bringing up said new server instance, or otherwise making available said new server instance to customers or other users of said first server.

4. (Original) The method of claim 1, further comprising bringing down said first server prior to said reprovisioning.

5. (Original) The method of claim 1, wherein said new server instance brought up in said reprovisioning differs from said first server in at least one parameter.

6. (Original) The method of claim 1, wherein a difference between said new server instance and said first server is responsive to whether or not other security incidents have been detected in a network to which said servers are coupled.

7. (Currently Amended) The method of claim 1, wherein a difference between said new server instance and said first server is responsive to a nature of any other security incidents that have been detected in ~~said~~ a network to which said servers are coupled.

8. (Original) The method of claim 1, wherein a difference between said new server instance and said first server is responsive to a probable compromise or a functional impairment observed in said detection.

9. (Original) The method of claim 1, wherein a difference between said new server instance and said first server includes a version of server software used by said servers.

10. (Original) The method of claim 1, wherein a difference between said new server instance and said first server includes a version of operating system software used by said servers.

11. (Original) The method of claim 1, wherein a difference between said new server instance and said first server includes a version of network connectivity software used by said servers.

12. (Currently Amended) The method of claim 1, wherein a difference between said new server instance and said first server includes a strength of encryption used by said servers.

13. (Original) The method of claim 1, wherein a difference between said new server instance and said first server includes a degree of function offered to users by said servers.

14. (Original) The method of claim 1, wherein said new server instance brought up in said reprovisioning differs from said first server only if more than a fixed number of instances of probable server compromise have been observed.

15. (Original) The method of claim 1, wherein a difference between said new server instance and said first server is responsive to a number of probable server compromises that have been observed.

16. (Currently Amended) The method of claim 1, wherein said first server comprises a computer providing services through a network.

17. (Currently Amended) The method of claim 1, wherein said first server comprises a program running on a network-coupled computer, providing services through a network.

18. – 22. (Cancelled)

23. (Currently Amended) A computer-readable medium having stored thereon a plurality of instructions for automated adaptive reprovisioning of servers under security assault, said plurality of instructions including instructions which, when executed by a processor, cause said processor to perform:

detecting a security assault or a possible security assault on a first server;

incrementing a counter associated with the first server to account for the security assault or possible security assault;

notifying a human operator if a value of said counter exceeds a maximum limit;

and

reprovisioning by automatically creating a new server instance with a ~~desired~~ new server configuration to perform at least one of the tasks performed by said first server, if said value of said counter does not exceed the maximum limit, wherein said ~~desired~~ new server configuration for said new server instance is selected from a table comprising a plurality of new server configurations ~~available for said first server~~ , said new server configuration being associated in said table with said value of said counter.

24. (Original) The computer-readable medium of claim 23, wherein said detecting comprises determining if said first server is a candidate for reprovisioning, because of properties or behavior that suggest its security has been compromised or is likely to be compromised, or its functioning otherwise unacceptably impaired, by a security assault.

25. (Original) The computer-readable medium of claim 23, wherein said reprovisioning comprises automatically bringing up said new server instance, or otherwise making available said new server instance to customers or other users of said first server.

26. (Original) The computer-readable medium of claim 23, further comprising bringing down said first server prior to said reprovisioning.

27. (Original) The computer-readable medium of claim 23, wherein said new server instance brought up in said reprovisioning differs from said first server in at least one parameter.

28. (Original) The computer-readable medium of claim 23, wherein a difference between said new server instance and said first server is responsive to whether or not other security incidents have been detected in a network to which said servers are coupled.

29. (Currently Amended) The computer-readable medium of claim 23, wherein a difference between said new server instance and said first server is responsive to a nature of any other security incidents that have been detected in ~~said~~ a network to which said servers are coupled.

30. (Currently Amended) A system for automated adaptive reprovisioning of servers under security assault, the system comprising:

a first server;

a counter associated with said first server, for tracking a number of times that said first server has come under security assault;

a security monitor, coupled to said first server, for detecting if said first server is a candidate for automatic reprovisioning with a new server instance having a ~~desired~~ new server configuration; ~~and~~

a table for storing a plurality of new server configurations, where each of said plurality of new server configurations corresponds to a potential value of said counter; and

a provisioner, coupled to said first server, for automatically reprovisioning said first server with said new server instance if said first server is such a candidate, wherein said ~~desired~~ new server configuration for said new server instance is selected from [[a]] the plurality of new server configurations ~~available for said first server~~ based on a current value of said counter.